Groups from cyclic infrastructures and Pohlig-Hellman in certain infrastructures

Fontein, F

Abstract: In discrete logarithm based cryptography, a method by Pohlig and Hellman allows solving the discrete logarithm problem efficiently if the group order is known and has no large prime factors. The consequence is that such groups are avoided. In the past, there have been proposals for cryptography based on cyclic infrastructures. We will show that the Pohlig-Hellman method can be adapted to certain cyclic infrastructures, which similarly implies that certain infrastructures should not be used for cryptography. This generalizes a result by Müller, Vanstone and Zuccherato for infrastructures obtained from hyperelliptic function fields. We recall the Pohlig-Hellman method, define the concept of a cyclic infrastructure and briefly describe how to obtain such infrastructures from certain function fields of unit rank one. Then, we describe how to obtain cyclic groups from discrete cyclic infrastructures and how to apply the Pohlig-Hellman method to compute absolute distances, which is in general a computationally hard problem for cyclic infrastructures. Moreover, we give an algorithm which allows to test whether an infrastructure satisfies certain requirements needed for applying the Pohlig-Hellman method, and discuss whether the Pohlig-Hellman method is applicable in infrastructures obtained from number fields. Finally, we discuss how this influences cryptography based on cyclic infrastructures.

DOI: https://doi.org/10.3934/amc.2008.2.293

GROUPS FROM CYCLIC INFRASTRUCTURES AND POHLIG-HELLMAN IN CERTAIN INFRASTRUCTURES

Felix Fontein
Institut für Mathematik
Universität Zürich
CH-8057, Switzerland
felix.fontein@math.uzh.ch

Abstract. In discrete logarithm based cryptography, a method by Pohlig and Hellman allows solving the discrete logarithm problem efficiently if the group order is known and has no large prime factors. The consequence is that such groups are avoided. In the past, there have been proposals for cryptography based on cyclic infrastructures. We will show that the Pohlig-Hellman method can be adapted to certain cyclic infrastructures, which similarly implies that certain infrastructures should not be used for cryptography. This generalizes a result by Müller, Vanstone and Zuccherato for infrastructures obtained from hyperelliptic function fields.

We recall the Pohlig-Hellman method, define the concept of a cyclic infrastructure and briefly describe how to obtain such infrastructures from certain function fields of unit rank one. Then, we describe how to obtain cyclic groups from discrete cyclic infrastructures and how to apply the Pohlig-Hellman method to compute absolute distances, which is in general a computationally hard problem for cyclic infrastructures. Moreover, we give an algorithm which allows to test whether an infrastructure satisfies certain requirements needed for applying the Pohlig-Hellman method, and discuss whether the Pohlig-Hellman method is applicable in infrastructures obtained from number fields. Finally, we discuss how this influences cryptography based on cyclic infrastructures.

1. Introduction

Since the advent of cryptographic protocols such as the Diffie-Hellman key exchange protocol and ElGamal encryption, the security of many cryptographic protocols is based on the hardness of the *discrete logarithm problem*: given h, an element of a finite cyclic group $\langle g \rangle$, find an integer $n \in \mathbb{N}$ such that $g^n = h$. In 1978, S. C. Pohlig and M. E. Hellman [20] presented an algorithm which allows to quickly solve the discrete logarithm problem in a finite cyclic group if the group order $|G|$ has a known factorization into a product of relatively small primes (see Section 4 for more details). Since then, one prefers to use groups of (almost) prime order or groups whose order has at least one large prime factor for discrete logarithm based cryptography, to avoid this kind of attack.

In 1990, R. Scheidler, J. A. Buchmann and H. C. Williams described a key exchange [5, 23], which was not based on cyclic groups but on a structure first

1991 *Mathematics Subject Classification.* Primary: 94A60, 14Q05; Secondary: 11Y99, 14G50, 14H45.

Key words and phrases. Infrastructures, Pohlig-Hellman, function fields, cryptography.

This work has been supported in part by the Swiss National Science Foundation under grant no. 107887.

introduced by D. Shanks in 1972 [28], called the *infrastructure* of a real quadratic number field. This structure behaves similar to finite cyclic groups, with the main difference that the operation corresponding to multiplication is not associative. This structure was generalized from real quadratic number fields to arbitrary number fields of unit rank one [6], and also to real quadratic function fields [33, 30, 32] and more general function fields [25, 22]. Moreover, the key exchange protocol for infrastructures was refined [13, 12] and extended to real quadratic function fields [26, 10]. The security of these protocols is mostly based on the fact that computing distances in infrastructures in general is assumed to be hard. As the problem of computing distances in infrastructures is related (see Section 5) to the problem of computing discrete logarithms in finite cyclic groups, one has to ask the question whether the idea of Pohlig-Hellman can be applied in this setting.

In 1998, V. Müller, S. Vanstone and R. Zuccherato [18] answered this question positively in the case of infrastructures obtained from real quadratic function fields of characteristic 2. We will generalize this to obtain a positive answer for a more general class of infrastructures, which includes all infrastructures obtained from function fields. Then, we will argue why this is probably not possible for infrastructures obtained from number fields, at least without further input.

In Section 2, we will define the concept of a cyclic infrastructure and show how such infrastructures can be obtained from certain global function fields with two infinite places. After that, in Section 3, we will show how to obtain cyclic groups from such infrastructures and how to efficiently compute in them, assuming that one can efficiently compute in the underlying infrastructure. In Section 4, we will recall how the Pohlig-Hellman method works, and in Section 5 we will show how Pohlig-Hellman can be applied in the case of discrete cyclic infrastructures. Then, in Section 6 we will describe an algorithm to test whether the main requirement of the Pohlig-Hellman method, namely that the group order is smooth, is satisfied. Finally, in Section 7, we will discuss the number field case, and in Section 8, we will explain the consequences for cyclic infrastructure based cryptography.

2. Cyclic infrastructures

In this section, we define an abstract version of a cyclic infrastructure. This definition, including the description of baby steps and giant steps, is based on the interpretation of Shanks' infrastructure in context of a 'circle group' by H. W. Lenstra [15], even though he uses a different distance function.

Roughly speaking, a cyclic infrastructure can be interpreted as a circle with a finite set of points on it.

Definition 2.1. Let $R \in \mathbb{R}_{>0}$ be a positive real number. A *cyclic infrastructure* (X, d) of *circumference* R is a non-empty finite set X with an injective map $d : X \to \mathbb{R}/R\mathbb{Z}$, called the *distance* function.

Definition 2.2. We say that a cyclic infrastructure (X, d) of circumference R is *discrete* if $R \in \mathbb{Z}$ and $d(X) \subseteq \mathbb{Z}/R\mathbb{Z}$.

One can interpret finite cyclic groups as discrete cyclic infrastructures as follows: Let $G = \langle g \rangle$ be a finite cyclic group of order m and $d : G \to \mathbb{Z}/m\mathbb{Z}$ be the *discrete logarithm* map[1] (to the base g), i.e. we have $g^{d(h)} = h$ for every $h \in \langle g \rangle$. By

[1]The discrete logarithm of an element $h \in \langle g \rangle$ is sometimes, in particular in Elementary Number Theory, also called the *index* of h with respect to g.

interpreting $\mathbb{Z}/m\mathbb{Z}$ as a subset of $\mathbb{R}/m\mathbb{Z}$, we get that (G, d) is a discrete cyclic infrastructure of circumference m.

An infrastructure has two operations, namely baby steps and giant steps. For their definition, we need the following notation:

Definition 2.3. Let $R \in \mathbb{R}_{>0}$ and let $x, y \in \mathbb{R}/R\mathbb{Z}$. Write $x = \hat{x} + R\mathbb{Z}$ and $y = \hat{y} + R\mathbb{Z}$ with $\hat{x}, \hat{y} \in \mathbb{R}$ such that $\hat{x} \leq \hat{y} < \hat{x} + R$. Define

$$[x, y] := \{t + R\mathbb{Z} \mid t \in \mathbb{R},\ \hat{x} \leq t \leq \hat{y}\}.$$

If one interprets $\mathbb{R}/R\mathbb{Z}$ as a circle with circumference R, and x and y as points on this circle, the set $[x, y]$ can be interpreted as the points on the circle which lie on the arc beginning at x and ending at y.

Now we can define baby steps and giant steps. We will exclude the case $|X| = 1$, as in this case the infrastructure is trivial and not of practical interest.

Proposition 1. *Let (X, d) be a cyclic infrastructure of circumference R. Assume that $|X| > 1$.*

(a) *Then there is a unique bijective fixed point free map* $\mathrm{bs} : X \to X$ *such that for every $x \in X$, we have*

$$[d(x), d(\mathrm{bs}(x))] \cap d(X) = \{d(x), d(\mathrm{bs}(x))\}.$$

This map is called baby step *map.*

(b) *Moreover, there is a unique map* $\mathrm{gs} : X \times X \to X$ *such that for every $x, y \in X$, we have*

$$[d(x) + d(y), d(\mathrm{gs}(x, y))] \cap d(X) = \{d(\mathrm{gs}(x, y))\}.$$

This map is called giant step *map.*

Let $G = \langle g \rangle$ be a finite cyclic group of order $n > 1$ and let $d : G \to \mathbb{Z}/n\mathbb{Z}$ be the discrete logarithm map. Then, for the cyclic infrastructure (G, d), we have $\mathrm{bs}(h) = gh$ and $\mathrm{gs}(h, h') = hh'$ for all $h, h' \in G$. Applying d, this translates to $d(\mathrm{bs}(h)) = d(h) + 1$ and $d(\mathrm{gs}(h, h')) = d(h) + d(h')$. This shows that baby and giant steps in arbitrary infrastructures generalize the group operation of a finite cyclic group.

In the case of finite cyclic groups, both baby steps and giant steps are basically the same operation. In arbitrary infrastructures, this is not the case, as in general there is no element $x \in X$ with $\mathrm{gs}(x, y) = \mathrm{bs}(y)$ for all $y \in X$.

In general, cyclic infrastructures behave similar to cyclic groups, with the main difference being that the giant step operation is not necessarily associative, but "almost" associative in the sense that

$$d(\mathrm{gs}(x, y)) \approx d(x) + d(y).$$

Here, "$\approx$" for elements in $\mathbb{R}/R\mathbb{Z}$ means that both sides have representatives in $\mathbb{R}$ which are relatively close to each other.

We want to close this section by showing how to obtain discrete cyclic infrastructures from certain global function fields. Let $\mathbb{F}_q$ be a finite field with q elements and $K = \mathbb{F}_q(x, y)$ a finite separable extension of $\mathbb{F}_q(x)$, x transcendental over $\mathbb{F}_q$, such that $\mathbb{F}_q$ is relatively algebraically closed in K. Let $\mathcal{O}$ be the integral closure of $\mathbb{F}_q[x]$ in K, and assume that the degree valuation of $\mathbb{F}_q(x)$ has exactly two extensions to K; these are the *infinite places* $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of K. Let $\nu_i : K \to \mathbb{Z} \cup \{\infty\}$ be the normalized valuation associated to $\mathfrak{p}_i$, $i = 1, 2$.

Now, by Dirichlet's Unit Theorem for function fields [16, p. 299, Theorem 9.5], $\mathcal{O}^* = \langle \varepsilon \rangle \oplus \mathbb{F}_q^*$ for some $\varepsilon \in \mathcal{O}^* \setminus \mathbb{F}_q^*$; without loss of generality, let $R := -\nu_1(\varepsilon) > 0$. Assume that **at least one of the infinite places has degree one**.[2]

If $a, b \in K^*$ are two elements, then the principal fractional ideals $\mathcal{O}a$ and $\mathcal{O}b$ are equal if, and only if, $\frac{a}{b} \in \mathcal{O}^*$. Therefore, if $\mathrm{PId}(\mathcal{O})$ denotes the set of non-zero principal fractional ideals of $\mathcal{O}$, we have a well-defined map

$$D : \mathrm{PId}(\mathcal{O}) \to \mathbb{Z}/R\mathbb{Z}, \qquad \mathcal{O}\frac{1}{a} \mapsto -\nu_1(a) + R\mathbb{Z}.$$

We say that a principal fractional ideal $\mathfrak{a} \in \mathrm{PId}(K)$ is *reduced* if $1 \in \mathfrak{a}$ and, for every $a \in \mathfrak{a} \setminus \{0\}$ with $\nu_i(a) \geq 0$, $i = 1, 2$, we must have $a \in \mathbb{F}_q^*$. Denote the set of all reduced principal fractional ideals by $\mathrm{Red}(K)$. Now one has that $d := D|_{\mathrm{Red}(K)}$ is injective,[3] which, in particular, shows that $X := \mathrm{Red}(K)$ is finite. Therefore, (X, d) is a discrete cyclic infrastructure.

In certain cases, namely real quadratic (i.e. real hyperelliptic) function fields [33, 32, 11] and for certain cubic function fields of unit rank one [25, 22], we can efficiently compute baby steps, inverse baby steps and giant steps (i.e. given $x, y \in X$, we can compute $\mathrm{bs}(x)$, $\mathrm{bs}^{-1}(x)$ and $\mathrm{gs}(x, y)$), and we can efficiently compute *relative distances*[4]

$$d(\mathrm{gs}(\mathfrak{a}, \mathfrak{b})) - d(\mathfrak{a}) - d(\mathfrak{b}) \qquad \text{and} \qquad d(\mathrm{bs}(\mathfrak{a})) - d(\mathfrak{a})$$

for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{Red}(K)$.

One further fundamental property of these infrastructures is that computation of d is hard, i.e. given $x \in X$, it is hard to compute the *absolute distance* $d(x)$ except for a few special values of x. Moreover, R itself does not need to be known. This allows to do cryptography in infrastructures, as for doing cryptography, one must be able to efficiently compute certain objects (here: baby steps, giant steps and relative distances), while inverse computations (here: computing absolute distances) must be hard.

3. Obtaining cyclic groups from discrete cyclic infrastructures

Our aim is to embed a cyclic infrastructure into a one-dimensional torus and to describe arithmetic on the torus using the arithmetic of the infrastructure, i.e. by using giant and baby steps. More precisely, we embed the infrastructure into $\mathbb{R}/R\mathbb{Z}$ or $\mathbb{Z}/R\mathbb{Z}$ by adding the missing elements that are not in the infrastructure. One way to describe these missing elements are f-representations.

In the number field case, another embedding and representation has been first described by H. W. Lenstra in [15]; a more general and more modern approach can be found in [27].

---

[2] If one drops this assumption, one cannot show that one has 'enough' reduced ideals, which makes computation of baby and giant steps problematic. One has to use another definition of reduced ideals, and define an equivalence relation on the set of all reduced ideals to make d injective.

[3] Let $\mathcal{O}\frac{1}{a}, \mathcal{O}\frac{1}{b} \in \mathrm{Red}(K)$ with $\nu_1(a) = \nu_1(b) + kR$, $k \in \mathbb{Z}$. As $\mathcal{O}\frac{1}{a} = \mathcal{O}\frac{1}{a\varepsilon^{-k}}$ and $\nu_1(a\varepsilon^{-k}) = \nu_1(b)$, we assume $k = 0$ without loss of generality. Now $\frac{b}{a} \in \mathcal{O}\frac{1}{a}$ and $\nu_1(\frac{b}{a}) = 0$. If $\nu_2(\frac{b}{a}) \geq 0$, then we must have $\frac{b}{a} \in \mathbb{F}_q^*$ as $\mathcal{O}\frac{1}{a}$ is reduced, whence $\mathcal{O}\frac{1}{a} = \mathcal{O}\frac{1}{b}$. If $\nu_2(\frac{b}{a}) < 0$, we have $\nu_2(\frac{a}{b}) > 0$, $\nu_1(\frac{a}{b}) = 0$ and $\frac{a}{b} \in \mathcal{O}\frac{1}{b}$, contradicting that $\frac{a}{b} \in \mathbb{F}_q^*$ as $\mathcal{O}\frac{1}{b}$ is reduced.

[4] From now on, we will interpret these relative distances as real numbers instead of elements of $\mathbb{R}/R\mathbb{Z}$, by identifying them with their smallest non-negative representative, i.e. we identify $a + R\mathbb{Z}$ with a if $0 \leq a < R$.

Let (X, d) be a cyclic infrastructure of circumference R.

Definition 3.1. An *f-representation* is a pair (x, f), where $x \in X$ and $f \in [0, R[$ such that $[d(x), d(x) + f] \cap d(X) = \{d(x)\}$. Denote the set of f-representations by $\mathrm{Rep}^f(X, d)$.

If (X, d) is discrete, define the subset

$$\mathrm{Rep}^f_{\mathrm{discrete}}(X, d) := \{(x, f) \in \mathrm{Rep}^f(X, d) \mid f \in \mathbb{Z}\}.$$

Note that infrastructures obtained from function fields, as described in Section 2, are discrete. One can also obtain infrastructures from number fields of unit rank one by a very similar method (for details, see [6]), but these are never discrete (see Section 7).

Definition 3.2. Define the *(absolute) distance* of a pair $(x, f) \in X \times \mathbb{R}$ by

$$d(x, f) := d(x) + f \in \mathbb{R}/R\mathbb{Z}.$$

Then we have the following proposition:

Proposition 2. *The map*

$$d|_{\mathrm{Rep}^f(X,d)} : \mathrm{Rep}^f(X, d) \to \mathbb{R}/R\mathbb{Z}, \qquad (x, f) \mapsto d(x, f) = d(x) + f$$

gives a bijection between the set of f-representations and $\mathbb{R}/R\mathbb{Z}$. If (X, d) is discrete, this restricts to a bijection

$$d|_{\mathrm{Rep}^f_{\mathrm{discrete}}(X,d)} : \mathrm{Rep}^f_{\mathrm{discrete}}(X, d) \to \mathbb{Z}/R\mathbb{Z}.$$

Remark 1. If $(x, f) \in X \times \mathbb{R}$ is arbitrary, there exists a *unique* f-representation (x', f') such that $d(x, f) = d(x', f')$. More precisely, it is the f-representation (x', f') with $d(x, f) = d(x', f')$ such that $f' \geq 0$ is minimal.

If $|f|$ is small, (x', f') can be computed efficiently using baby steps by starting with (x, f) and minimizing f:

(1) While f is negative, replace (x, f) by $(\mathrm{bs}^{-1}(x), f + \Delta)$, where $\Delta := d(x) - d(\mathrm{bs}^{-1}(x)) \in [0, R[$.
(2) Compute $x'' := \mathrm{bs}(x)$ and $\Delta' := d(x'') - d(x) \in [0, R[$.
(3) If $\Delta' > f$, then (x, f) is an f-representation and we are done.
(4) Otherwise, replace (x, f) by $(x'', f - \Delta')$ and continue with step (2).

One quickly sees that all operations do not modify the distance $d(x, f)$. In case (X, d) is discrete, one needs at most $|f|$ (inverse) baby step computations.

Using this remark, we get the following proposition:

Proposition 3. *If (x, f) and (x', f') are f-representations, consider the tuple*

$$(\mathrm{gs}(x, x'), f + f' - (d(\mathrm{gs}(x, x')) - d(x) - d(x'))).$$

By the previous remark, it corresponds to a unique f-representation (x'', f''). If we define

$$(x, f) \circ (x', f') := (x'', f''),$$

we get that $(\mathrm{Rep}^f(X, d), \circ)$ is a group and

$$d|_{\mathrm{Rep}^f(X,d)} : (\mathrm{Rep}^f(X, d), \circ) \to (\mathbb{R}/R\mathbb{Z}, +)$$

is a group isomorphism. If (X, d) *is discrete, we get that* $(\mathrm{Rep}^f_{\mathrm{discrete}}(X,d), \circ)$ *is a subgroup of* $\mathrm{Rep}^f(X,d)$ *and that*

$$d|_{\mathrm{Rep}^f_{\mathrm{discrete}}(X,d)} : (\mathrm{Rep}^f_{\mathrm{discrete}}(X,d), \circ) \to (\mathbb{Z}/R\mathbb{Z}, +)$$

is a group isomorphism. The relationships between these structures are described in the following diagram:

$$\begin{array}{ccccc} X \times \mathbb{R} & \supsetneq & \mathrm{Rep}^f(X,d) & \supsetneq & \mathrm{Rep}^f_{\mathrm{discrete}}(X,d) \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle \cong\, d|_{\mathrm{Rep}^f(X,d)}} & & \downarrow{\scriptstyle \cong\, d|_{\mathrm{Rep}^f_{\mathrm{discrete}}(X,d)}} \\ \mathbb{R}/R\mathbb{Z} & = & \mathbb{R}/R\mathbb{Z} & \supsetneq & \mathbb{Z}/R\mathbb{Z} \end{array}$$

Therefore, if we are able to effectively compute bs, bs^{-1} and gs and relative distances for an infrastructure (X, d), we can efficiently compute in a group isomorphic to $\mathbb{R}/R\mathbb{Z}$ or $\mathbb{Z}/R\mathbb{Z}$, even if R is unknown and without the need to evaluate the function d for general elements of X. More precisely:

Corollary 1. *Let* (X, d) *be an infrastructure such that* bs, bs^{-1} *and* gs *are efficiently computable, together with the relative distances. Let* $d_{\min} := \min\{d(\mathrm{bs}(x)) - d(x) \mid x \in X\}$ *and* $d_{\max} := \max\{d(\mathrm{bs}(x)) - d(x) \mid x \in X\}$. *Then one group operation in* $\mathrm{Rep}^f(X,d)$ *can be computed using one* gs *computation and at most* $\left\lceil \frac{2d_{\max}}{d_{\min}} \right\rceil$ *computations of* bs *or at most* $\left\lceil \frac{d_{\max}}{d_{\min}} \right\rceil$ *computations of* bs^{-1}.

Proof. Given $(x, f), (x', f') \in \mathrm{Rep}^f(X, f)$, one first computes (x'', f'') by $x'' := \mathrm{gs}(x, x')$ and $f'' := f + f' + (d(x) + d(x') - d(x''))$; then $d(x'', f'') = d(x, f) + d(x', f')$. As, by definition of the giant step function, $-d_{\max} < d(x) + d(x') - d(x'') \leq 0$, we have $-d_{\max} < f'' < 2d_{\max}$. When replacing (x'', f'') by $(\mathrm{bs}(x''), f'' - (d(\mathrm{bs}(x'')) - d(x'')))$ resp. $(\mathrm{bs}^{-1}(x''), f'' + (d(x'') - d(\mathrm{bs}^{-1}(x''))))$, we have that f'' decreases resp. increases at least by $d_{\min}$. Hence, we can do at most $\left\lceil \frac{2d_{\max}}{d_{\min}} \right\rceil$ baby steps resp. $\left\lceil \frac{d_{\max}}{d_{\min}} \right\rceil$ inverse baby steps before f'' gets negative resp. positive. □

If (X, d) is a discrete infrastructure, $d_{\min} \geq 1$. If (X, d) is obtained from a function field as described at the end of Section 2, it is an easy application of the Riemann-Roch Theorem [34, p. 28, Theorem I.5.15] to see that $d_{\max} \leq \left\lceil \frac{g + \deg \mathfrak{p}_2}{\deg \mathfrak{p}_1} \right\rceil$. This also shows that one should order $\mathfrak{p}_1$ and $\mathfrak{p}_2$ such that $\deg \mathfrak{p}_1 \geq \deg \mathfrak{p}_2$. Note that this result is also valid if $\deg \mathfrak{p}_i > 1$ for both i.

Remark 2. In case we want to compute in $\mathrm{Rep}^f(X,d)$ (which is, for example, necessary if (X, d) is not discrete), we need to work with (arbitrary) real numbers. As this is not possible on computers, one needs to approximate them using floating point numbers. More details on this can be found in [9] and [13]; there, such representations are called CRIAD-representations resp. (f, p)-representations.

Finally, we want to note that in the case of real hyperelliptic function fields, a similar representation has been used by S. Paulus and H.-G. Rück in [19] to describe the arithmetic in the Jacobian. This, together with the discussion in [11], shows that in this case, our group $\mathbb{Z}/R\mathbb{Z}$ is in fact the subgroup of the Jacobian which is generated by the divisor class of $\mathfrak{p}_1 - \mathfrak{p}_2$. This is also true for non-hyperelliptic function fields under the assumption that $\deg \mathfrak{p}_1 = \deg \mathfrak{p}_2 = 1$.

4. Pohlig-Hellman in groups

Before explaining how to do Pohlig-Hellman in discrete infrastructures in Section 5, we want to recall the Pohlig-Hellman method for finite cyclic groups.

Assume that we have a finite cyclic group $G = \langle g \rangle$ of order m and an element $h \in G$. We can consider the *discrete logarithm problem*, which states that one wants to find some $n \in \mathbb{N}$ with

$$g^n = h.$$

Note that n is unique modulo m. Assume that the prime factorization

$$m = \prod_{i=1}^{t} p_i^{e_i}$$

with distinct primes $p_1, \dots, p_t$ and positive integers $e_1, \dots, e_t \in \mathbb{N}_{>0}$ is known. To compute n, note that by the Chinese Remainder Theorem,

$$G \cong \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{e_t}\mathbb{Z}.$$

Therefore, we can compute n modulo $p_i^{e_i}$ for every i and deploy the Chinese Remainder Theorem to recover n modulo m.

To compute $n \bmod p_i^{e_i}$, we successively compute $n \bmod p_i^{\ell}$, $\ell = 1, \dots, e_i$, by considering the discrete logarithm problem

$$\left(g^{m/p_i^{\ell}}\right)^{n \bmod p_i^{\ell}} = h^{m/p_i^{\ell}},$$

where $n \bmod p_i^{\ell}$ is sought. As we assume that we already know $n \bmod p_i^{\ell-1}$, we only have to solve the discrete logarithm problem

$$\left(g^{m/p_i}\right)^{n'} = h^{m/p_i^{\ell}} g^{-m/p_i^{\ell} \cdot (n \bmod p_i^{\ell-1})}, \tag{1}$$

where $n' \in \{0, \dots, p_i - 1\}$, to obtain

$$n \bmod p_i^{\ell} = (n \bmod p_i^{\ell-1}) + n' p_i^{\ell-1}.$$

Assuming that we are using a method for solving discrete logarithms for elements of prime order p which needs $\mathcal{O}(\sqrt{p})$ group operations (according to [29], this is optimal if one assumes that G behaves like a generic group), the running time of Pohlig-Hellman is

$$\mathcal{O}\Big(\sum_{i=1}^{t} e_i \max\{\sqrt{p_i}, \log m\}\Big) = \mathcal{O}\big(t \max_{i=1,\dots,t} e_i \max\{\sqrt{p_i}, \log m\}\big)$$

group operations.

5. Pohlig-Hellman in discrete infrastructures

Assume that (X, d) is a discrete infrastructure of circumference $R \in \mathbb{Z}$. We have seen that this gives rise to a finite set $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$ of R elements, which can be equipped with the structure of a cyclic group. In the following, we will write this group *additively*, i.e. the group operation will be $+$ and instead of exponentiation, we will use scalar multiplication.

We further assume that R together with an element $(x, f) \in \mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$ is known where $d(x, f) = d(x) + f$ is known and small.[5] Using baby steps and inverse

[5]We call an element $r \in \mathbb{R}/R\mathbb{Z}$ *small* if we can write $r = \hat{r} + R\mathbb{Z}$ with $\hat{r}$ small.

baby steps, we can compute an f-representation (x', f') with $d(x', f') = 1$ from this (compare Remark 1). Then we have $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d) = \langle (x', f') \rangle$.

In the group $(\mathrm{Rep}^f_{\mathrm{discrete}}(X, d), +)$ we can consider the *discrete logarithm problem*

$$n \cdot (x', f') = (x'', f''),$$

where $(x'', f'') \in \mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$ and $n \in \mathbb{Z}$. In particular, as $d(x', f') = 1$, we have that $d(x'', f'') = n + R\mathbb{Z}$, whence solving the discrete logarithm problem for an element in X is *equivalent* to computing a distance of an element in X.

As we can effectively compute the group operation in $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$, we can employ any algorithm for computing discrete logarithms in groups to find n and, in particular, as we know the group order, we can employ the Pohlig-Hellman algorithm.

Assume that the prime factorization

$$R = \prod_{i=1}^{t} p_i^{e_i}$$

with distinct primes $p_1, \ldots, p_t$ and positive integers $e_1, \ldots, e_t \in \mathbb{N}_{>0}$ is known. We have seen in Section 4 that in order to find n, we need to solve the discrete logarithm problems

$$n' \cdot \left(\frac{R}{p_i} \cdot (x', f') \right) = \frac{R}{p_i^\ell} \cdot (x'', f'') - (n \bmod p_i^{\ell-1}) \cdot \left(\frac{R}{p_i^\ell} \cdot (x', f') \right) \tag{2}$$

for n' for $i = 1, \ldots, t$ and $\ell = 1, \ldots, e_i$; this is Equation (1) transcribed to our setting. Note that we know that the order of $\frac{R}{p_i^\ell} \cdot (x', f')$ divides p_i^ℓ, whence we have that $-\frac{R}{p_i^\ell} \cdot (x', f') = (p_i^\ell - 1) \cdot \frac{R}{p_i^\ell} \cdot (x', f')$. In particular, there is no need to compute inverses, if one rewrites Equation (2) as

$$n' \cdot \left(\frac{R}{p_i} \cdot (x', f') \right) = \frac{R}{p_i^\ell} \cdot (x'', f'') + (n \bmod p_i^{\ell-1}) \cdot (p_i^\ell - 1) \cdot \left(\frac{R}{p_i^\ell} \cdot (x', f') \right).$$

As in Section 4, we get that the running time of Pohlig-Hellman is

$$\mathcal{O}\Big(\sum_{i=1}^{t} e_i \max\{\sqrt{p_i}, \log R\} \Big) = \mathcal{O}\big(t \max_{i=1,\ldots,t} e_i \max\{\sqrt{p_i}, \log R\} \big)$$

group operations in $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$.

Remarks 1.

(a) The Pohlig-Hellman method can be parallelized: for computing $n \bmod p_i^{e_i}$, there is no knowledge required of $n \bmod p_j^{e_j}$ for any $j \neq i$. This reduces the running time to

$$\mathcal{O}\big(\max_{i=1,\ldots,t} e_i \max\{\sqrt{p_i}, \log R\} \big)$$

group operations in $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$ when using t processors.

(b) Note that it suffices to know an *integer multiple* R' of the circumference R and the factorization

$$R' = \prod_{i=1}^{t'} p_i^{\hat{e}_i}$$

with $t' \geq t$. In this case, we have $\hat{e}_i \geq e_i$ for each $i \leq t$. If one applies Pohlig-Hellman with R' instead of R, i.e. by replacing the e_i's by the $\hat{e}_i$'s,

the algorithm will return the same value of n, as for $\ell > e_i$, the solution of Equation (2) will be $n' = 0$. The only disadvantage is that the running time will increase to

$$\mathcal{O}\big(t' \max_{i=1,\dots,t} \hat{e}_i \max\{\sqrt{p_i}, \log R\}\big)$$

group operations.

An alternative is to first try to find the e_i's from the $\hat{e}_i$'s. For that, one computes $\frac{R'}{p_i} \cdot (x', f')$ for each i; if this equals the identity in $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$, we have $\hat{e}_i > e_i$. In that case, we can decrease $\hat{e}_i$ by one, i.e. replace R' by $\frac{R'}{p_i}$, and try again.

(c) One can also deploy the Pohlig-Hellman method if $d(x', f') \neq 1$. In case no n' is found for one instance of Equation (2), we have $(x'', f'') \notin \langle (x', f') \rangle$.

If we have $d(x', f') \neq 1$, it is enough to know an integer multiple of $\frac{R}{\gcd(\ell, R)}$, where $\ell \in \mathbb{Z}$ is any integer with $\ell + R\mathbb{Z} = d(x', f')$, as $\frac{R}{\gcd(\ell, R)}$ is the order of (x', f') in $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$.

6. Testing for smooth circumference

With respect to the result from last section, it is desirable to check whether a given discrete cyclic infrastructure (X, d) with circumference R satisfies that R is B-smooth, i.e. that all prime divisors of R are $\leq B$, for some integer $B \in \mathbb{N}$. In practice, in particular when using a discrete cyclic infrastructure for cryptographic reasons, it can happen that R is not known. In this section, we present an algorithm which still allows to check whether R is B-smooth. (Also see the discussion following Question 1 in Section 8, where the smoothness of the regulator of a randomly chosen function field is discussed.)

For this, we make the following requirements:

(1) we know some $(x, f) \in \mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$ with $d(x, f) = 1$;
(2) we know an upper bound R' for R;
(3) for every $(x', f') \in \mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$, we can efficiently check whether $d(x', f') = 0$, i.e. whether (x', f') is the identity in $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$.

For discrete cyclic infrastructures obtained from unit rank one function fields as described in Section 2, these requirements are always satisfied. Assume that K is such a function field with full field of constants $\mathbb{F}_q$ and genus g. Then we have that:

(1) either $(x, f) = (\mathcal{O}, 1)$ or $(x, f) = (\mathrm{bs}(\mathcal{O}), 0)$ is an f-representation with $d(x, f) = 1$;
(2) an explicit upper bound for R can be given using Hasse-Weil, as shown below; and
(3) $d(x', f') = 0$ if, and only if, $x' = \mathcal{O}$ and $f' = 0$.

Both (1) and (3) follow from the fact that $d(\mathcal{O}) = 0$ and from the definition of f-representations. For (2), let $d = \gcd(\deg \mathfrak{p}_1, \deg \mathfrak{p}_2)$ and $D := \frac{\deg \mathfrak{p}_2}{d}\mathfrak{p}_1 - \frac{\deg \mathfrak{p}_1}{d}\mathfrak{p}_2 \in \mathrm{Div}(K)$. Then, for $n = \left|\mathrm{Pic}^0_{\mathbb{F}_q}(K)\right|$, the divisor nD is principal. Now, by Hasse-Weil, $n \leq (1 + \sqrt{q})^{2g}$ [16, p. 287, Corollary 6.3 and Remark 6.4]. As $nD \neq 0$ must be the divisor of a non-constant unit ε of $\mathcal{O}$, we obtain

$$R \leq |\nu_1(\varepsilon)| \leq \frac{\deg \mathfrak{p}_2}{d}(1 + \sqrt{q})^{2g}.$$

Note that this bound is rather crude; for example, for real quadratic function fields of Richaud-Degert type, the regulator is very small.

Our method is formulated in the following lemma:

Lemma 6.1. *Let $p_1, \ldots, p_t$ be all primes $\leq B$, and define*

$$m := \prod_{i=1}^{t} p_i^{\left\lfloor \frac{\log R'}{\log p_i} \right\rfloor},$$

where R' satisfies $R' \geq R$. Then R is B-smooth if, and only if, $d(m \cdot (x, f)) = 0$.

Proof. Firstly, note that R is B-smooth if, and only if, $R \mid m$, as $R \leq R'$. Secondly, the cyclic group $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$ is generated by (x, f) and has order R, whence $m \cdot (x, f)$ is the identity (i.e. has distance 0) if, and only if, m is an integer multiple of R. □

Note that our method is very similar to the computations done in J. Pollard's $(p-1)$-method [17, p. 93, Algorithm 3.14] or in H. W. Lenstra's Elliptic Curve Method for Factorization [14].

Remark 3. To evaluate $m \cdot (x, f)$, one can proceed iteratively, as it is usually done in Pollard's $(p-1)$-method and in Lenstra's Elliptic Curve Method:

Define $(x_0, f_0) := (x, f)$ and

$$(x_i, f_i) := p_i^{\left\lfloor \frac{\log R'}{\log p_i} \right\rfloor} (x_{i-1}, f_{i-1}), \qquad 1 \leq i \leq t.$$

Then $m \cdot (x, f) = (x_t, f_t)$. To compute (x_i, f_i) from (x_{i-1}, f_{i-1}), one does $\left\lfloor \frac{\log R'}{\log p_i} \right\rfloor$ consecutive multiplications of (x_{i-1}, f_{i-1}) by p_i.

Therefore, to compute $m \cdot (x, f)$ using this method, one needs

$$\mathcal{O}\Big(t \left\lfloor \tfrac{\log R'}{\log p_i} \right\rfloor \log p_i\Big) = \mathcal{O}(t \log R')$$

group operations in $\mathrm{Rep}^f(X, d)$, assuming a square-and-multiply technique is used for multiplication by p_i.

In the case of infrastructures obtained from function fields, we get:

Corollary 2. *If (X, d) is a discrete infrastructure of circumference R obtained from a function field (as in Section 2) of genus g with full field of constants $\mathbb{F}_q$, then one needs at most $\mathcal{O}(tg \log q)$ giant step and $\mathcal{O}(tg^2 \log q)$ baby step computations to check whether R is p_t-smooth, where p_t is the t-th prime number.*

7. Pohlig-Hellman and infrastructures based on number fields

In the case that K is a number field of unit rank one, i.e. with two places at infinity, one can construct a cyclic infrastructure basically the same way as for function fields with two places at infinity. This is, for example, described in [6]. In the number field case, $\mathcal{O}$ is the integral closure of $\mathbb{Z}$ in K, and $\mathbb{F}_q^*$ is replaced by the roots of unity in K. The places at infinity correspond to the (non-conjugate) embeddings $K \to \mathbb{C}$; if the two embeddings are σ_1 and σ_2, the condition that $\deg \sigma_i = 1$ for one i corresponds to $\sigma_i(K) \subseteq \mathbb{R}$. Moreover, the valuations ν_i are defined by $\nu_i(x) := -\log |\sigma_i(x)|$, $x \in K^*$. Let (X, d) be the resulting infrastructure.

Note that if $\alpha \in K^*$, then $|\sigma_i(\alpha)|$ is algebraic over $\mathbb{Q}$ and, hence, $\nu_i(\alpha)$ is transcendental over $\mathbb{Q}$ by Lindemann's Theorem if $\nu_i(\alpha) \neq 0$. Therefore, in particular,

neither R nor any element of $d(X)$, except 0, is a rational number, whence (X,d) is far from being discrete.

Let $x \in \mathcal{O} \setminus \{0\}$. We want to investigate when $\frac{\nu_1(x)}{R} \in \mathbb{Q}$ happens. If $R = \nu_1(\varepsilon)$ for $\varepsilon \in \mathcal{O}^*$, we have that $\frac{\nu_1(x)}{R} = \frac{p}{q}$ with $p, q \in \mathbb{Z} \setminus \{0\}$ implies $|\sigma_1(x^q/\varepsilon^p)| = 1$. By [3, p. 285, (8)], we must have $|\sigma_2(x^q/\varepsilon^p)| = 1$. Now, if $\mathcal{O}\frac{1}{x}$ is reduced, this implies that $\frac{x^q}{\varepsilon^p}$ is a root of unity, i.e. is equal to ± 1, i.e. we have that $x^q = \pm\varepsilon^p$. But then, we have

$$N_{K/\mathbb{Q}}(x)^q = N_{K/\mathbb{Q}}(x^q) = N_{K/\mathbb{Q}}(\pm\varepsilon^p) = \pm 1,$$

whence our assumption $x \in \mathcal{O}$ implies that $x \in \mathcal{O}^*$. This is the main ingredient of the following result:

Proposition 4. *If $\mathfrak{a} \in \mathrm{Red}(K)$, then $(\mathfrak{a}, 0)$ has finite order in $\mathrm{Rep}^f(X,d)$ if, and only if, $\mathfrak{a} = \mathcal{O}$.*

Proof. If $\mathfrak{a} = \mathcal{O}$, then $(\mathfrak{a}, 0)$ is the identity of $\mathrm{Rep}^f(X,d)$. For the other direction, write $\mathfrak{a} = \mathcal{O}\frac{1}{x}$ with $x \in \mathcal{O}$. As $d : \mathrm{Rep}^f(X,d) \to \mathbb{R}/R\mathbb{Z}$, $(\mathfrak{b}, f) \mapsto d(\mathfrak{b}) + f = -\nu_1(x) + f + R\mathbb{Z}$ is an isomorphism, $(\mathfrak{a}, 0)$ having finite order means that $\frac{-\nu_1(x)}{R} \in \mathbb{Q}$. By the discussion before the lemma, this implies $x \in \mathcal{O}^*$, whence $\mathfrak{a} = \mathcal{O}\frac{1}{x} = \mathcal{O}$. □

As the Pohlig-Hellman method (or any other of the standard discrete logarithm problem solvers) requires an element of finite order (of which an integer multiple has to be known in the case of the Pohlig-Hellman method), we cannot directly apply the Pohlig-Hellman method to $(\mathfrak{a}, 0) \in \mathrm{Rep}^f(X,d)$, but have to find a positive real number $f \in \mathbb{R}$ and an f-representation $(\mathfrak{b}, f') \in \mathrm{Rep}^f(X,d)$ with $d(\mathfrak{a}) + f = d(\mathfrak{b}) + f'$ such that $(\mathfrak{b}, f')$ has finite order in $\mathrm{Rep}^f(X,d)$.

This of course opens the question how to find such an f, if one does not already know $d(\mathfrak{a})$ and R. Obviously, if one knows $d(\mathfrak{a})$ in advance, there is no need to apply the Pohlig-Hellman method to compute $d(\mathfrak{a})$. Hence, one has to find f without this information, or one has to adjust the Pohlig-Hellman method to circumvent this problem.

Finally, as Lenstra used a different distance function in the case that K is a real quadratic number field [15], we want to investigate whether with his distance function, a Pohlig-Hellman variant is possible. Let K be a real quadratic number field and let σ be the unique non-trivial automorphism of K. Assume that $\mathcal{O}\frac{1}{x} \in \mathrm{Red}(K)$.

Instead of using the distance $-\nu_1(x) + R\mathbb{Z}$, Lenstra uses $\frac{1}{2}(\nu_2(x) - \nu_1(x)) + R\mathbb{Z} = \frac{1}{2}\log\left|\frac{\sigma_1(x)}{\sigma_2(x)}\right| + R\mathbb{Z}$. Then, $\frac{\nu_2(x)-\nu_1(x)}{2R} = \frac{p}{2q} \in \mathbb{Q}$ is equivalent to $\frac{\sigma_1(x^q)}{\sigma_1(\sigma(x)^q)} = \frac{\sigma_1(x^q)}{\sigma_2(x^q)} = \pm\sigma_1(\varepsilon^{-p})$ for $p, q \in \mathbb{Z}$, $q \neq 0$. Now $\sigma(x^q) = \pm x^q \varepsilon^{-p}$ means that if $\mathfrak{p}$ is a finite place of K, then $q\nu_{\mathfrak{p}}(x) = q\nu_{\sigma(\mathfrak{p})}(x)$. But this means that $\frac{\sigma(x)}{x} \in \mathcal{O}^*$, which implies $\varepsilon^{-p/q} \in \mathcal{O}^*$. Since $\mathcal{O}^* = \langle -1, \varepsilon\rangle$, it follows that $\frac{p}{q} \in \mathbb{Z}$. Without loss of generality, assume $q = 1$, i.e. we have $\frac{\nu_2(x)-\nu_1(x)}{2R} = \frac{p}{2}$. Hence, $\frac{\nu_2(x)-\nu_1(x)}{2} + R\mathbb{Z}$ can attain at most the values $0 + R\mathbb{Z}$ and $\frac{R}{2} + R\mathbb{Z}$ in $\mathbb{R}/R\mathbb{Z}$, whence by [15, p. 15, Section 10] there are at most two f-representations $(\mathcal{O}\frac{1}{x}, 0) \in \mathrm{Rep}^f(X,d)$ of finite order, and the possible orders are one or two.

By this argumentation, we have the same problems implementing Pohlig-Hellman using this distance function as in the case of the other distance function.

8. Conclusion

There exist several cryptosystems employing discrete cyclic infrastructures; for examples of such, see [4, 23, 26, 13, 12, 10]. They are all based on the hardness of computing distances: if (X, d) is a cyclic infrastructure, these systems require that it is hard to compute $d(x)$ for a general $x \in X$. Note that this is equivalent to computing $d(x, 0)$ for $(x, 0) \in \mathrm{Rep}^f(X, d)$.

Now assume that (X, d) is discrete with circumference R, and that an integer multiple R' of R is known. Moreover, assume that R' is smooth, i.e. that R' factors with relatively small prime factors. If baby, inverse baby and giant steps and relative distances can be computed efficiently, we can use the Pohlig-Hellman method described in Section 5 to compute $d(x, 0)$ relatively fast.

Hence, in order for cryptosystems which are based on the hardness of computing absolute distances in discrete cyclic infrastructures to be safe, one has to use discrete infrastructures such that

(a) either it is very hard to compute a multiple R' of R which can be factorized,
(b) or R is not smooth, i.e. has at least one very large prime factor.

In (a), it may even be enough that only a part of R' can be factorized, if this part is still a multiple of R: assume that R' factors as $R_1 R_2$, where R_1 is smooth, i.e. has small prime factors, but R_2 has only very large prime factors. Then it still might be that R_2 is not needed for computing $d(x)$: one computes $R_1 \cdot (\mathcal{O}, 1)$, and if it equals $(\mathcal{O}, 0)$, one can take R_1 instead of R. If one knows that R is smooth, R will be a divisor of R_1 and we will have $R_1 \cdot (\mathcal{O}, 1) = (\mathcal{O}, 0)$.

To avoid the possibility that the Pohlig-Hellman method can be used, one has to use function fields whose regulator is not B-smooth for a "large enough" B. A naïve way to find such function fields is to randomly pick a function field (with two places at infinity, one of them of degree one) and to apply the algorithm from Section 6 to check whether the regulator is B-smooth; this procedure is repeated until a sufficient curve is found.

This leads to several important questions:

(1) How smooth is the regulator of an average function field with two places at infinity, one of them of degree one?

In [26, Section 6.1], R. Scheidler, A. Stein and H. C. Williams apply the heuristic arguments of H. Cohen and H. W. Lenstra to real hyperelliptic function fields. They reason that the odd part of the ideal class group $\mathrm{Pic}(\mathcal{O})$ of $\mathcal{O}$ in the real hyperelliptic function field case is small with high probability. As $R \cdot |\mathrm{Pic}(\mathcal{O})| = \left|\mathrm{Pic}^0_{\mathbb{F}_q}(K)\right|$, and $\left|\mathrm{Pic}^0_{\mathbb{F}_q}(K)\right| \in [(\sqrt{q}-1)^{2g}, (\sqrt{q}+1)^{2g}]$, this shows that R is large with high probability. More importantly, the smoothness of R is more or less equivalent to the smoothness of $\left|\mathrm{Pic}^0_{\mathbb{F}_q}(K)\right|$ under the assumption of these heuristics.

An equivalent to the Cohen-Lenstra heuristics for quadratic number fields is the heuristics by E. Friedman and L. C. Washington [8] for quadratic function fields. The main difference to the number field case is that for function fields, these have been proven (in a slightly modified version) by J. D. Achter [1] in certain cases. In our case, an older result by J. D. Achter and J. Holden [2] already gives sufficient information. Let ℓ be a prime which is coprime to q. Then, by [2, Lemma 3.3], the proportion of real hyperelliptic function fields K of genus g over $\mathbb{F}_q$ for which $\ell \nmid \left|\mathrm{Pic}^0_{\mathbb{F}_q}(K)\right|$ is $1 - \frac{\ell}{\ell^2-1} + \mathcal{O}(1/\ell^3)$ if $\ell \equiv 1 \pmod{q}$ and $1 - \frac{1}{\ell-1} + \mathcal{O}(1/\ell^3)$ if $\ell \not\equiv 1$

(mod q). This is slightly less than the probability that a random natural number in the interval $[(\sqrt{q}-1)^{2g}, (\sqrt{q}+1)^{2g}]$ is not divisible by ℓ, which is approximately $1-\frac{1}{\ell}$.

Therefore, one expects that R is B-smooth with a slightly higher probability than that a random natural number in the interval $[(\sqrt{q}-1)^{2g}, (\sqrt{q}+1)^{2g}]$ is B-smooth, which is rather low for $B \ll q^g$.

A more straightforward approach to the problem of finding function fields whose regulator is not B-smooth would be to ask the following question:

(2) Can one *efficiently* construct function fields with two places at infinity, one of them of degree one, such that the regulator is known to have a very large prime factor?

More generally, one can also ask the following question:

(3) Given an arbitrary positive integer R, can one efficiently construct a function field with two places at infinity, one of them of degree one, which has regulator R, or $R \cdot \ell$ with $\ell \in \mathbb{N}$ small?

In the case of real elliptic function fields, this is basically equivalent to finding an elliptic curve together with a rational point of order R, as it is explained in [31]: if E is an elliptic curve over $\mathbb{F}_q$ with the point ∞ at infinity, and if $P \in E(\mathbb{F}_q) \setminus \{\infty\}$, one can transform the equation of E such that one obtains a function field with two places at infinity, which correspond to the two points P and ∞ of E. Moreover, the regulator of this new function field is exactly the order of P, and the reduced principal ideals correspond to the multiples of P. For hyperelliptic function fields, one has a similar correspondence; see [19].

Currently, elliptic or hyperelliptic curves (or, more precisely, their imaginary function field counterparts K) with a specific number of points (i.e. elements in $\mathrm{Pic}^0_{\mathbb{F}_q}(K)$) are usually constructed using complex multiplication, or by choosing curves from very special families of curves (see, for example, [7]). It is currently not known whether there are special attacks for these classes of curves.

A final question arises from the fact that there are also proposals for cyclic infrastructure based cryptography for infrastructures obtained from number fields (for examples, see [5, 23, 13, 12]). In the previous section, we have seen that the Pohlig-Hellman method cannot be applied in the number field case in its current state. Therefore, one can ask the following:

(4) Can a similar method be applied to cyclic infrastructures obtained from number fields, or generally to non-discrete cyclic infrastructures?

So far, the author is not aware of any idea of whether this question can be answered positively.

Acknowledgments

I would like to thank Renate Scheidler for the suggestion to consider the Pohlig-Hellman method for infrastructures, Michael J. Jacobson, Jr. for pointing me to H. W. Lenstra's paper and Andreas Stein, Joachim Rosenthal, Jeffrey D. Achter and the anonymous referees for their valuable comments and suggestions. Moreover, I would like to thank the Institut für Mathematik at the Carl von Ossietzky Universität Oldenburg for their hospitality during my stay.

References

[1] J. D. Achter, *The distribution of class groups of function fields*, J. Pure Appl. Algebra, **204** (2006), 316–333.

[2] J. D. Achter and J. Holden, *Notes on an analogue of the Fontaine-Mazur conjecture*, J. Théor. Nombres Bordeaux, **15** (2003), 627–637.

[3] H. Appelgate and H. Onishi, *Periodic expansion of modules and its relation to units*, J. Number Theory, **15** (1982), 283–294.

[4] I. Biehl, J. A. Buchmann and C. Thiel, *Cryptographic protocols based on discrete logarithms in real-quadratic orders*, in "Advances in Cryptology—CRYPTO '94" (ed. Y. Desmedt), Springer, (1994), 56–60.

[5] J. A. Buchmann and H. C. Williams, *A key exchange system based on real quadratic fields (extended abstract)*, in "Advances in cryptology—CRYPTO '89 (Santa Barbara, CA, 1989)," Springer, (1990), 335–343.

[6] J. A. Buchmann and H. C. Williams, *On the infrastructure of the principal ideal class of an algebraic number field of unit rank one*, Math. Comp., **50** (1988), 569–579.

[7] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren, "Handbook of Elliptic and Hyperelliptic Curve Cryptography," Chapman & Hall/CRC, 2005.

[8] E. Friedman and L. C. Washington, *On the distribution of divisor class groups of curves over finite fields*, in "Theorie des Nombres, Proc. Int. Number Theory Conf. Laval, 1987", Walter de Gruyter, (1989), 227–239.

[9] D. Hühnlein and S. Paulus, *On the implementation of cryptosystems based on real quadratic number fields (extended abstract)*, in "Selected Areas in Cryptography (Waterloo, ON, 2000)", Springer, (2001), 288–302.

[10] M. J. Jacobson, R. Scheidler and A. Stein, *Cryptographic protocols on real hyperelliptic curves*, Adv. Math. Commun., **1** (2007), 197–221.

[11] M. J. Jacobson, R. Scheidler and A. Stein, *Fast arithmetic on hyperelliptic curves via continued fraction expansions*, in "Advances in Coding Theory and Cryptography" (eds. T. Shaska, W.C. Huffman, D. Joyner and V. Ustimenko), World Scientific Publishing Co. Pte. Ltd., **3** (2007), 201–245.

[12] M. J. Jacobson, R. Scheidler and H. C. Williams, *An improved real-quadratic-field-based key exchange procedure*, J. Cryptology, **19** (2006), 211–239.

[13] M. J. Jacobson, R. Scheidler and H. C. Williams, *The efficiency and security of a real quadratic field based key exchange protocol*, in "Public-key Cryptography and Computational Number Theory (Warsaw, 2000)," Walter de Gruyter, (2001), 89–112.

[14] H. W. Lenstra, *Factoring integers with elliptic curves*, Ann. of Math. (2), **126** (1987), 649–673.

[15] H. W. Lenstra, *On the computation of regulators and class numbers of quadratic fields*, in "Journées Arithmétiques 1980 (Exeter, 13th–19th April 1980)," Cambridge University Press, (1982), 123–150.

[16] D. Lorenzini, "An Invitation to Arithmetic Geometry," American Mathematical Society, Providence, RI, 1996.

[17] A. J. Menezes, P. van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, FL, 1997.

[18] V. Müller, S. Vanstone and R. Zuccherato, *Discrete logarithm based cryptosystems in quadratic function fields of characteristic 2*, Des. Codes Cryptogr., **14** (1998), 159–178.

[19] S. Paulus and H.-G. Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Math. Comp., **68** (1999), 1233–1241.

[20] S. C. Pohlig and M. E. Hellman, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE Trans. Inform. Theory, **24** (1978), 106–110.

[21] M. I. Rosen, "Number Theory in Function Fields," Springer, New York, 2002.

[22] R. Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields*, J. Théor. Nombres Bordeaux, **13** (2001), 609–631.

[23] R. Scheidler, J. A. Buchmann and H. C. Williams, *A key-exchange protocol using real quadratic fields*, J. Cryptology, **7** (1994), 171–199.

[24] R. Scheidler and A. Stein, *Class number approximation in cubic function fields*, Contrib. Discrete Math., **2** (2007), 107–132.

[25] R. Scheidler and A. Stein, *Unit computation in purely cubic function fields of unit rank 1 (extended abstract)*, in "Proceedings of the Third Algorithmic Number Theory Symposium ANTS-III" (ed. J. Buhler), Springer, (1998), 592–606.

[26] R. Scheidler, A. Stein and H. C. Williams, *Key-exchange in real quadratic congruence function fields*, Des. Codes Cryptogr., **7** (1996), 153–174.

[27] R. Schoof, *Computing Arakelov class groups*, in "Surveys in Algorithmic Number Theory," Cambridge University Press, (2008), 447–495.

[28] D. Shanks, *The infrastructure of a real quadratic field and its applications*, in "Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972)", Univ. Colorado, (1972), 217–224.

[29] V. Shoup, *Lower bounds for discrete logarithms and related problems*, in "Advances in Cryptology—EUROCRYPT '97" (ed. W. Fumy), Springer, (1997), 256–266.

[30] A. Stein, "Baby step-giant step-Verfahren in reellquadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich 2," M.Sc. thesis, Universität des Saarlandes in Saarbrücken, 1992.

[31] A. Stein, *Equivalences between elliptic curves and real quadratic congruence function fields*, J. Théor. Nombres Bordeaux, **9** (1997), 75–95.

[32] A. Stein, *Infrastructure in real quadratic function fields*, Technical Report CORR 99-17, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, May 1999.

[33] A. Stein and H. G. Zimmer, *An algorithm for determining the regulator and the fundamental unit of hyperelliptic congruence function field*, in "Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ISSAC '91", Association for Computing Machinery, (1991), 183–184.

[34] H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, Berlin Heidelberg, 1993.